

REMARKS

Claims 1 – 4, 6 – 14, 16 – 19, and 21 – 27 have been examined. Claims 1, 23, and 27 stand rejected under the second paragraph of 35 U.S.C. §112 for use of the word “suspect”; Claims 1, 16, 17, 23, 24, and 27 stand rejected under 35 U.S.C. §101 as directed to nonstatutory subject matter; and Claims 1 – 4, 6 – 14, 16 – 19, and 21 – 27 stand rejected under 35 U.S.C. §103(a) as unpatentable over U.S. Pat. No. 5,892,900 (“Ginter”).

1. §112 Rejections

Applicants respectfully disagree with the assertion in the Office Action that the term “suspect” is not an accepted term in the art, particularly in light of the fact that the claims include a definition of the term by limiting such phrases as “suspect money transfer requests” to a defined set circumstances (*see, e.g.*, Claim 1, ll. 18 – 33). See MPEP 2111.01.III permitting Applicants to act as their own lexicographers. Nevertheless, in the interest of advancing prosecution of the application, the claims have been amended to substitute uses of the word “suspect” with “suspicious,” an equivalent term also used in the specification (*see, e.g.*, Application, p. 2, ll. 30 – 31). Such amendments do not alter the scope of the claims.

Claim 17 has been amended to add the definition used in others of the independent claims. Since all independent claims now include such explicit definitions, the phrases used in the claims are well-defined and withdrawal of the §112 rejections is respectfully requested.

2. §101 Rejections

The §101 rejections are respectfully traversed. On September 28, 2005, the Board of Patent Appeals and Interferences (“the Board”) held in a precedential decision that “there is currently no judicially recognized separate ‘technological arts’ test to determine patent eligible

subject matter under §101.” *Ex Parte Lundgren*, 76 USPQ2d 1385, 1388 (BPAI 2005). The Office Action acknowledges that “the recited process produces a useful, concrete, and tangible result” (Office Action, p. 4). Since the §101 rejections are thus otherwise grounded only in a position of the Office that has been rejected by the Board, the rejections are respectfully believed to be improper, and withdrawal of the rejections is accordingly requested.

3. §103 Rejections

The prior-art rejections under §103 are respectfully traversed. Applicants note their general disagreement with the Office Action’s characterization of the claims as “articulated [to] read on any electronic transaction method in which transactions are grouped or batched according to various characteristics in order to differentiate fraudulent from nonfraudulent transaction” (Office Action, p. 4). The claims recite detailed specific limitations and such a characterization of them improperly attempts to identify a gist of the invention: “Distilling an invention down to the ‘gist’ or ‘thrust’ of an invention disregards the requirement of analyzing the subject matter ‘as a whole.’ ” MPEP 2141.02.II.

Nevertheless, in the interest of continuing to advance prosecution of the Application, the following observations are made regarding the cited art in light of this characterization. The Office Action cites only a single reference, Ginter, which provides a comprehensive description of particular systems and methods for electronic commerce. While there is some discussion of fraud detection in this document, it is very limited and fails to disclose the claimed methods and systems for evaluating electronic value transfers.

The Office Action cites two specific portions of Ginter, with a caution that the document should be considered in its entirety. First, the Office Action cites the following:

Some of the key factors contributing to the configurability intrinsic to the present invention include:

(a) integration into the fundamental control environment of a broad range of electronic appliances through portable API and programming language tools that efficiently support merging of control and auditing capabilities in nearly any electronic appliance environment while maintaining overall system security;

- (b) modular data structures;
- (c) generic content model;
- (d) general modularity and independence of foundation architectural components;
- (e) modular security structures;
- (f) variable length and multiple branching chains of control; and
- (g) independent, modular control structures in the form of executable load modules that can be maintained in or more libraries, and assembled into control methods and models, and where such model control schemes can "evolve" as control information passes through the VDE installations of participants of a pathway of VDE content control information handling.

Because of the breadth of issues resolved by the present invention, it can provide the emerging "electronic highway" with a single transaction/distribution control system that can, for a very broad range of commercial and data security models, ensure against unauthorized use of confidential and/or proprietary information and commercial electronic transactions.
(Ginter, Col. 16, l. 62 – Col. 17, l. 24).

This disclosure is unrelated to differentiating fraudulent from nonfraudulent transactions. It merely describes at a high level certain characteristics of the "virtual distribution environment" ("VDE") that is the focus of Ginter. While Applicants readily acknowledge that the factors identified in the cited passage are of value to the VDE arrangement that Ginter proposes, they are respectfully believed not to be relevant to the claims because they do not disclose specific features of evaluating electronic value transfers nor of discriminating between potentially fraudulent and nonfraudulent transactions.

Second, the Office Action cites the following:

A further usage map could be maintained to detect fraudulent usage of the same object. For example, the object might be stored in such a way that sequential access of long blocks should never occur. A METER method could then record all applicable atomic elements accesses during, for example, any specified increment of time, such as ten minutes, an hour, a day, a month, a year, or any other time duration). The usage map could be analyzed at the end of the specified time increment to check for an excessively long contiguous set of accessed blocks, and/or could be analyzed at the initiation of each access to applicable atomic elements. After each time duration based analysis, if no fraudulent use is detected, the usage map could be cleared (or partially cleared) and the mapping process could begin in whole or in part anew. If a fraudulent use pattern is suspected or detected, that information might be recorded and the use of the object could be halted. For example, the user might be required to contact a content provider who might then further analyze the usage information to determine whether or not further access should be permitted.
(Ginter, Col. 154, ll. 20 – 40).

Although this disclosure is related to the detection of fraud, it is of a completely different character than what is claimed. The technique described is applicable to monitoring a

user's access to some kind of object, with an example being described in Ginter of an electronic novel (*see id.*, Col. 152, l. 63 – Col. 153, l. 18). The “fraudulent” access occurs when access of that object is improper. The cited passage describes how analysis of access patterns of the object can be used to identify when the access may be improper. The technique does not group different transactions according to various criteria, but simply performs the analysis on a particular usage. Indeed, the passage teaches away from the Office Action's characterization of the claims by explicitly teaching that each fraud analysis be performed independently: “After each time duration based analysis, if no fraudulent use is detected, the usage map could be cleared (or partially cleared) and the mapping process could begin in whole or in part anew” (*id.*, Col. 154, ll. 31 – 34).

Importantly, none of the cited passages is related to transfers of electronic value, which is central to the claims: there is no disclosure of receiving a plurality of money transfer requests, no disclosure of electronically storing records of money transfer requests, no disclosure of performing an analysis of money transfer requests to indicate a relationship between sender identifications, no disclosure of creation of a reference designator associated with the sender identifications, and no disclosure of searching records of money transfer requests to determine if any associated with a reference designator are suspicious as defined by the explicit criteria in the claims. Since these elements are not taught or suggested by the cited art, the claims are respectfully believed to be patentable. MPEP 2143.

Mindful of the Office Action's request to consider the reference in its entirety, the reference has been examined for other suggestions of fraud identification. There are several such suggestions, but it is believed that none of them teach or suggest the specific limitations of the claims. For example, the disclosure at Col. 152, ll. 29 – 39 relates to an object having an atomic element type that may relate to fraud detection; this disclosure does not teach or suggest the collection and analysis of money transfer requests recited in the claims. The disclosure at Col. 174, l. 52 – Col. 175, l. 6 notes that copies of backup files may be used to check for indications of fraudulent activity; this disclosure does not teach or suggest the collection and analysis of money transfer requests recited in the claims. The disclosure at Col. 230, ll. 43 – 54 indicates that activity patterns like excessive acquisition of protected content without payment as

uncovered by a consistency check may be indicative of fraud; this disclosure does not teach or suggest the collection and analysis of money transfer requests recited in the claims. The disclosure at Col. 313, ll. 9 – 21 again indicates broadly that usage patterns may aid in fraud detection, but fails to teach or suggest the collection and analysis of money transfer requests recited in the claims. The disclosure at Col. 318, ll. 30 – 58 is also related to analysis of usage patterns, but like other such disclosures in Ginter does not teach or suggest the collection and analysis of money transfer requests recited in the claims.


For the above reasons, each of the independent claims is believed to be patentably distinguishable from the cited art, and the dependent claims are believed to be patentable by virtue of their dependence from patentable claims.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 303-571-4000.

Respectfully submitted,


Patrick M. Boucher
Reg. No. 44,037

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 303-571-4000
Fax: 415-576-0300
PMB:pmb
60659109 v1